Preparing for Quantum Technologies: Key Considerations for Financial Sector Participants

Report prepared by the G7 Central Bank Quantum Technologies Working Group co-chaired by the Banque de France and the Bank of Canada

May 2026

Foreword

Quantum technologies are progressing from fundamental research toward early forms of deployment, prompting growing attention across public institutions, financial authorities and the broader technology ecosystem. These developments raise important questions for the financial system, particularly in areas where trust, security, resilience and long-term stability are critical.

This publication is a public adaptation of analytical work conducted within the framework of cooperation among G7 central banks. It builds on collective expertise developed through research activities, technical experimentation and ongoing dialogue with academic and institutional partners. The objective of this public version is to make available a shared analytical foundation on the implications of quantum technologies for finance, while ensuring clarity, neutrality and accessibility for a wider audience.

The report is intended for financial-sector stakeholders, public institutions and policy makers, as well as informed audiences within the quantum and cybersecurity ecosystem. It aims to contribute to a common understanding of both risks and opportunities associated with quantum technologies, to support informed discussion, and to serve as a reference point for dialogue across institutional and sectoral boundaries.

This contribution does not seek to anticipate regulatory decisions, promote specific policy approaches, or prescribe courses of action. Given the rapid pace of technological change and the uncertainty surrounding future developments, the analysis deliberately avoids speculative assertions on timelines or outcomes that are not grounded in established research and observable trends. Instead, it emphasizes factual analysis, clearly identified uncertainties, and the trade-offs inherent in different technological pathways.

By sharing this work publicly, the contributing institutions aim to foster transparency and constructive engagement on a topic of growing relevance for the financial system. A well-informed and balanced public discourse is an essential condition for preparedness, coordination and trust as quantum technologies continue to evolve.

Executive Summary

Quantum technologies, including quantum computing, quantum communication and quantum sensing, are transitioning from predominantly academic research into early stages of experimentation and deployment. While many applications remain exploratory, these developments are increasingly relevant for a financial system reliant on secure data, trusted communications and complex computation.

This report examines two areas where quantum technologies may have material implications for finance. The first concerns **data and communication security**, in light of advances in quantum computing that are expected, over time, to challenge widely used cryptographic techniques underpinning digital trust. The second focuses on **potential applications of quantum technologies**

across financial markets, payment systems and central banking activities, as well as their broader system-level effects.

With respect to security, expert assessments suggest a **non-negligible probability that a cryptographically relevant quantum computer could emerge** over the coming decade, although no such system currently exists. In parallel, the possibility of "harvest-now, decrypt-later" attacks highlight the importance of long-term data confidentiality, particularly for information that must remain secure well beyond current cryptographic lifecycles. These considerations underscore why quantum-related risks are increasingly incorporated into discussions on financial system resilience.

Several quantum-safe approaches are being developed to address these challenges. **Post-quantum cryptography, supported by international standardisation efforts, is emerging as a central element of the transition toward quantum-resilient security**. The implementation of post-quantum cryptography is, however, not a simple substitution exercise. In practice, migration efforts may require inventorying cryptographic dependencies, testing compatibility with existing systems, and coordinating updates with external counterparties and service providers. This is the core position of the G7 Cyber Expert Group (CEG), who are supporting the coordination of post-quantum cryptography following the publication of its roadmap for transitioning to quantum-safe technologies in January 2026. Other approaches, including quantum-based communication techniques and symmetric key distribution architectures, may complement cryptographic solutions in specific contexts. These other options involve trade-offs related to technological maturity, scalability, interoperability, operational complexity and cost, suggesting that no single approach is universally applicable.

Beyond security, quantum technologies may also influence how financial systems operate. Research and early experimentation indicate that **quantum computing techniques could, over time, outperform conventional computers for certain computational tasks relevant to finance, such as optimisation, simulation and risk analysis**. Potential areas of impact include financial markets, payment and settlement systems, and analytical functions (e.g. macroeconomic simulations, financial stability modelling or large-scale stress testing) within central banks and financial institutions. At the same time, the adoption of advanced quantum capabilities may introduce new forms of dependency, concentration and shared vulnerabilities.

The implications of quantum technologies extend beyond individual use cases, raising broader considerations related to governance, resilience and skills. Adoption is likely to remain uneven across institutions and jurisdictions, reflecting technological maturity and access to expertise.

Taken together, these elements highlight the importance of a structured and fact-based understanding of quantum technologies and their potential effects on the financial system. Clarifying impacts, risks and trade-offs can support informed dialogue among financial-sector stakeholders, public institutions and the wider quantum and cybersecurity communities as these technologies continue to evolve.

Introduction

As quantum technologies are shifting from research to early deployments, their implications for the global financial and economic landscape are becoming increasingly tangible. Although many capabilities remain under development, progress in quantum computing, quantum communication and quantum sensing has prompted increased attention from public institutions, financial authorities and market participants. For the financial system, these developments raise questions that extend beyond technological performance, touching on trust, security, resilience and long-term stability.

Financial systems rely on digital infrastructures whose integrity depends on secure communications, robust cryptographic mechanisms and the ability to process and analyse large volumes of data. **Quantum technologies intersect with these foundations in multiple ways**. On the one hand, advances in quantum computing may, over time, undermine certain cryptographic techniques that currently support confidentiality, authentication and data integrity. On the other hand, quantum-based methods may also eventually enhance secure communication and data transfer, as well as certain computational tasks relevant to finance, including optimisation, simulation and modelling.

This report focuses on the implications of quantum technologies where they are most directly relevant to the functioning of the financial system. It examines two priority areas. The first concerns **data and communication security**, which remains a cornerstone of trust in financial infrastructures and institutions. The second explores **potential applications of quantum technologies in finance**, including their possible effects on financial markets, payment and settlement systems, and analytical functions within central banks and financial institutions.

Quantum technologies encompass three distinct but interrelated domains: quantum computing, quantum communication, and quantum sensing. Quantum computing exploits quantum mechanical properties to address specific classes of computational problems that are difficult to solve with classical computers. Quantum communication[1] leverages physical principles of quantum mechanics to enable new approaches to secure information exchange. Quantum sensing uses quantum effects to achieve highly precise measurements of physical quantities such as time, magnetic fields or electromagnetic signals. Each of these domains may affect financial systems in different ways and are at different stages of maturity.

In light of these developments, **the objective of this report is to provide a structured analytical framework to support understanding of quantum-related risks, opportunities and trade-offs relevant to the financial system**. Rather than advancing predictions or policy positions, it seeks to clarify areas where quantum technologies intersect with financial infrastructures and activities, and to highlight considerations that may shape future developments.

[1] A quantum communications channel based on quantum key distribution is secure from an information-theoretic perspective. In cryptography, information-theoretic means that the security cannot be breached even if the adversary possesses unlimited amounts of compute, memory and time. However, end-to-end security in practical deployments also depends on classical components, implementation choices and operational controls, which may introduce additional vulnerabilities.

By focusing on factual analysis and clearly identified uncertainties, **the report aims to contribute to informed discussion among financial-sector stakeholders, public institutions and the broader quantum and cybersecurity communities**. A shared understanding of these issues can support constructive dialogue and enhance collective preparedness as quantum technologies continue to evolve.

Focus Domain 1: Data and Communication Security

The security of data and communications is a foundational element of trust in the financial system. Financial infrastructures rely on cryptographic mechanisms to ensure confidentiality, integrity, authentication and non-repudiation across a wide range of activities, from payment processing and settlement to supervisory reporting and cross-border information exchange.

Advances in quantum technologies introduce new considerations for this security framework. While quantum-enabled capabilities remain at different stages of maturity, their potential to affect existing cryptographic assumptions has prompted increased attention across the financial sector. This section examines how quantum technologies intersect with data and communication security, focusing on the nature of the emerging threat landscape, the implications for long-term confidentiality, and the range of technical approaches being explored to enhance quantum resilience.

The analysis in this domain does not assume a specific technological trajectory or timeline. Instead, it provides a structured overview of risks, uncertainties and trade-offs relevant to financial infrastructures, with the objective of supporting informed assessment and dialogue.

1.1 Quantum Development Timeline

The prospect of quantum-enabled threats to data and communication security is primarily associated with advances in quantum computing. Certain cryptographic algorithms widely used today—particularly those underpinning public-key encryption and digital signatures—are based on mathematical problems that are believed to be intractable for classical computers. Research has demonstrated, however, that sufficiently powerful quantum computers could solve some of these problems much more efficiently, thereby undermining the security assumptions on which current cryptographic systems rely.

At present, no cryptographically relevant quantum computer capable of breaking commonly deployed encryption schemes exists. Nonetheless, **expert assessments and surveys indicate a growing expectation that such capabilities could emerge over the coming decade**. Estimates vary widely, reflecting substantial uncertainty regarding scientific progress, engineering constraints, scalability challenges and potential advances in quantum algorithm design and optimisation. These assessments do not imply inevitability within a fixed timeframe, but they do suggest that **quantum-related risks are no longer purely theoretical, particularly when considering the combined effects of hardware progress and algorithmic improvements**.

An important additional dimension of the threat landscape arises from the temporal characteristics of sensitive data. In many financial and institutional contexts, information must remain confidential for

extended periods, sometimes decades. This creates exposure to so-called “harvest-now, decrypt-later” scenarios, in which encrypted data is intercepted and stored today with the intention of decrypting it in the future once more advanced computational capabilities become available. Financial infrastructures and institutions exchange a wide range of data that may be affected by these dynamics. This includes communications between financial institutions and market infrastructures, interactions with central banks and public authorities, and data supporting payment systems, settlement processes and supervisory functions.

Beyond confidentiality, similar temporal considerations apply to cryptographic mechanisms supporting authentication, integrity and non-repudiation. If digital signature schemes currently in use were to become vulnerable to sufficiently advanced quantum computing capabilities, this could, over time, enable the forgery of signatures or impersonation of trusted entities. Emerging digital financial technologies, including tokenised assets, digital identity frameworks and distributed ledger-based systems, rely extensively on cryptographic mechanisms for authentication, integrity and non-repudiation[2]. As such, their long-term robustness may also be affected if quantum-related vulnerabilities are not addressed in a timely manner.

While such scenarios depend on the emergence of cryptographically relevant quantum computing capabilities, they illustrate that quantum-related risks concern not only the protection of stored data, but also the long-term robustness of trust mechanisms underpinning digital financial infrastructures.

The potential impacts of such vulnerabilities may extend beyond individual systems or institutions. Compromised confidentiality, forgery of digital signatures, impersonation of trusted entities, or the manipulation of transaction data could undermine confidence in financial infrastructures and, if sustained, affect broader trust in the financial system. These risks are not unique to quantum technologies, but quantum computing introduces a distinct class of challenges by targeting cryptographic foundations rather than implementation flaws or operational weaknesses.

1.2 Cryptographic transition and quantum-safe approaches

Post-quantum cryptography or PQC[3] refers to a new class of cryptographic algorithms designed to remain secure against attacks enabled by quantum computers, while being implementable on classical computing infrastructures. These algorithms aim to replace or complement widely deployed public-key cryptographic schemes whose security could be challenged by sufficiently advanced quantum computers.

Modern digital security relies on two core cryptographic functions: key establishment, which allows parties to agree on shared secrets over untrusted networks, and digital signatures, which ensure authentication, integrity and non-repudiation of data and transactions. Several of the public-key

[2] A digital signature is a mathematical guarantee that the content originated from a particular source and has not been tampered with in any way before arriving at its destination. It also ensures that the sender cannot claim to have not sent the message after the fact.

[3] Post-quantum cryptography (PQC) refers to the development of cryptographic algorithms that are designed to remain secure against attacks conducted by quantum computers.

algorithms currently used for these purposes are based on mathematical problems that are believed to be extremely time consuming for classical computers but could be efficiently solved by quantum algorithms under certain conditions. Post-quantum cryptographic schemes are designed around alternative mathematical foundations that are not known to be vulnerable to such quantum-enabled attacks.

International standardisation efforts play a central role in the development and evaluation of post-quantum cryptography. In particular, the National Institute of Standards and Technology (NIST) has led a multi-year, open and competitive process to assess candidate algorithms, resulting in the selection and standardisation of several post-quantum schemes for key establishment and digital signatures. These standards are progressively being incorporated into cryptographic libraries, software stacks and security products, providing a technical basis for broader adoption across sectors.

From a financial-system perspective, post-quantum cryptography is often viewed as a pragmatic and scalable approach to enhancing quantum resilience, as it can, in principle, be deployed over existing communication networks and infrastructure. At the same time, transitioning to post-quantum cryptographic algorithms involves a range of technical and operational considerations. These include performance impacts, increased key and signature sizes, integration with legacy systems, and the need to ensure interoperability across institutions and jurisdictions during potentially extended transition periods.

The implementation of post-quantum cryptography is therefore not a simple substitution exercise. Financial infrastructures are highly interconnected, and cryptographic mechanisms are deeply embedded across hardware, software, protocols and operational processes. In practice, migration efforts may require inventorying cryptographic dependencies, testing compatibility with existing systems, and coordinating updates with external counterparties and service providers. During transitional phases, systems using different cryptographic standards may need to coexist, raising additional challenges related to interoperability and operational complexity.

Post-quantum cryptography also interacts with broader questions of cryptographic agility and governance. Given ongoing research and the evolving nature of both classical and quantum cryptanalysis, the ability to adapt cryptographic mechanisms over time is an important consideration. This includes maintaining flexibility to update algorithms, parameters and implementations as standards evolve or as new information emerges about their security properties.

Overall, post-quantum cryptography represents a key component of the emerging set of quantum-safe security approaches. Its development and standardisation reflect a collective effort by the global cryptographic community to address long-term risks associated with quantum computing, while acknowledging that implementation choices involve trade-offs and uncertainties that must be carefully assessed in context.

The recent work conducted within the G7 Cyber Expert Group (CEG) has further examined the practical dimensions of the transition toward post-quantum cryptography. The *G7 CEG Quantum Readiness*

Roadmap outlines key activities that organisations may consider when preparing for this transition, including the identification of cryptographic dependencies, risk assessment, migration planning and the implementation of cryptographic agility. Additional details are available in the roadmap published by the G7 CEG[4].

In addition to post-quantum cryptography, **other complementary approaches are being explored** to enhance quantum resilience in specific contexts. These include Distributed Symmetric Key Exchange (DSKE) architectures, which rely on coordinated symmetric key distribution models, and Quantum Key Distribution (QKD), which leverages quantum communication techniques to establish cryptographic keys under alternative security assumptions. **While differing in maturity, deployment requirements and operational implications, these approaches illustrate that quantum-safe security does not rely on a single technological pathway**. A more detailed overview of these complementary options is provided in Appendix 1.

1.3 Data Security beyond cryptography

While cryptographic mechanisms are central to securing data and communications, quantum technologies also raise security considerations that extend beyond encryption and key exchange alone. As quantum-enabled capabilities are explored for computation, communication and sensing, new interfaces, architectures and operational models emerge, each introducing distinct security and resilience questions.

One area of interest concerns the protection of data during computation. As quantum computing resources are expected to be accessed primarily through cloud-based or remote platforms, sensitive data may need to be processed outside the direct control of the data owner. This has led to growing attention on techniques often described as confidential or blind quantum computing. These approaches aim to ensure that data and computational intent remain hidden from the quantum service provider, even while computations are being performed.

In classical computing, analogous objectives are pursued through technologies such as trusted execution environments and fully homomorphic encryption, which allow computation on encrypted data at the cost of additional complexity and performance overhead. In quantum contexts, research explores how quantum states and protocols may be used to limit the information exposed to the computing platform. While these approaches are conceptually promising, they remain largely experimental and are subject to significant technical constraints. In practice, hybrid architectures combining classical and quantum components introduce multiple points where data may be exposed, requiring careful consideration of end-to-end security.

The interfaces between classical and quantum systems represent another important area of focus. Quantum processors do not operate in isolation; they depend on classical control systems, data pipelines, storage and communication channels. These classical components may remain vulnerable to conventional cyber threats, even if the quantum operations themselves benefit from intrinsic physical

[4] G7-CEG-Quantum-Roadmap.pdf

protections. As a result, overall system security depends not only on the properties of quantum devices, but also on the robustness of the surrounding classical infrastructure, information security program, and the integrity of interactions between components.

Quantum sensing technologies introduce a further set of considerations. Quantum sensors exploit quantum effects to achieve extremely high precision in measuring physical quantities such as time, electromagnetic fields or magnetic signals. Some applications of quantum sensing are already deployed in domains such as timekeeping and navigation, which underpin elements of financial infrastructure, including transaction timestamping and synchronisation. Enhanced precision may support improvements in system integrity and monitoring.

At the same time, advances in quantum sensing may give rise to new risks. Increased sensitivity could enable forms of measurement or surveillance that challenge existing assumptions about privacy, detectability or interference resistance. For example, the ability to detect weak electromagnetic signals or operate in environments resistant to jamming could have implications for secure communications and data protection. These developments remain at varying levels of maturity, but they highlight that quantum-related security considerations are not limited to cryptographic algorithms alone.

Overall, developments beyond cryptography underscore the importance of viewing quantum security in a holistic manner. Protecting data and communications in a quantum-enabled environment involves not only selecting appropriate cryptographic primitives, but also understanding system architectures, trust boundaries, operational dependencies and emerging sensing capabilities. As research and experimentation continue, these broader dimensions will play an increasingly important role in assessing how quantum technologies interact with the security foundations of the financial system.

1.4 Cross-cutting considerations

The security implications of quantum technologies for data and communications extend beyond individual technologies or use cases. They are shaped by a set of cross-cutting factors that influence how quantum-safe approaches are assessed, deployed and sustained across complex financial infrastructures. The table below summarises these key dimensions. Further analytical detail is provided in Appendix 2.

Cross-cutting dimension	Key issues	Implications for the financial system
Interoperability and transition complexity	Coexistence of legacy and quantum-safe systems; integration across jurisdictions and infrastructures; embedded cryptographic dependencies in protocols and workflows	Extended transition phases may require parallel operation of multiple security standards, increasing complexity and coordination challenges
Operational dependencies and third-party	Reliance on vendors, service providers and specialised infrastructure; concentration risk; supply-chain	Security technology choices may influence dependency structures and resilience to disruption; security

risk (not specific to quantum)	exposure; the relation of any dependencies to critical functions	capabilities, expertise, and costs may correlate to service provider scale
Cryptographic agility and governance	Need to update algorithms, parameters and implementations over time; architectural flexibility; institutional decision processes	Effective governance and coordination mechanisms are critical to managing long-term cryptographic evolution
Skills and operational readiness	Scarcity of interdisciplinary expertise; inventory of cryptographic dependencies; capacity to manage complex transitions	Differences in skills and resources may shape the pace and scope of adoption across institutions

Focus Domain 2: Applications of Quantum Technologies in the Financial Sector

Beyond their implications for data and communication security, **quantum technologies may also influence how certain functions within the financial system are performed**. Advances in quantum computing have prompted growing interest in potential applications related to certain computation-intensive tasks, such as optimisation, simulation and data analysis. These applications remain at an exploratory or experimental stage, but their possible relevance for finance has become an area of active research and discussion.

This domain examines how quantum technologies may interact with financial markets, payment and settlement systems, and analytical and operational functions within central banks and financial institutions. **The analysis considers both potential efficiency gains and the broader system-level implications that may arise as quantum-enabled capabilities are explored or adopted**. Particular attention is given to issues of maturity, scalability and integration with existing infrastructures, as well as to the dependencies and risks that may accompany new computational paradigms.

Importantly, the development and adoption of quantum applications in finance do not occur in isolation. They intersect with broader trends in digitalisation, including advances in high-performance computing, artificial intelligence and cloud-based services. As a result, many near-term use cases involve hybrid approaches that combine classical and quantum resources. Understanding these interactions is essential for assessing where quantum technologies may add value, where they may introduce new vulnerabilities, and where their impact is likely to remain limited in the foreseeable future.

This section does not forecast the widespread deployment of quantum applications in finance, nor does it prioritise specific use cases. Rather, **it seeks to provide a structured overview of areas where quantum technologies are being explored and to clarify the nature of potential impacts**. By doing so, it aims to support informed assessment and dialogue on how quantum technologies may, over time, shape aspects of the financial system. To be clear, at present, application of quantum technology to financial sector issues is only at an experimental stage, as the technology has not advanced to a point where practical application is feasible or cost-effective.

2.1 Quantum Techniques of Interest

Quantum computing differs from classical computing in the way information is represented and processed. Instead of operating solely on binary states, quantum computers rely on quantum bits, or qubits[5], which can encode and manipulate information using quantum mechanical properties. This enables certain types of calculations to be approached in fundamentally different ways compared to classical architectures.

Quantum processors are not general-purpose replacements for classical computers. Rather, they are specialised devices designed to address specific classes of mathematical problems. In this respect, quantum processing units can be compared to other specialised computing accelerators, such as graphics processing units, which are widely used today for tasks like numerical simulation or machine learning. The potential relevance of quantum computing for finance therefore depends on whether financial problems can be formulated in ways that benefit from these specialised capabilities. Research has identified several categories of computational problems where quantum approaches may offer advantages under certain conditions.

For readers seeking a more technical overview, Appendix 3 provides a non-exhaustive table of prominent quantum algorithms frequently discussed in the literature, together with their primary computational characteristics and areas of relevance.

2.1.1. Mathematical Methods

A number of quantum algorithms focus on accelerating core mathematical operations, such as matrix inversion or the solution of systems of linear equations[6]. These operations play an important role in financial modelling, risk analysis and optimisation routines. In theory, certain quantum algorithms could perform these tasks more efficiently than classical methods for specific problem structures. In practice, however, the applicability of such algorithms depends on factors including data preparation costs, error rates and the scale of available quantum hardware.

Quantum approaches to statistical sampling have also attracted attention. Sampling from complex probability distributions is a common requirement in financial applications, particularly in stochastic modelling and Monte Carlo simulations. Quantum techniques may enable alternative sampling strategies that are difficult to replicate classically, although translating these theoretical advantages into practical gains remains an open research question.

2.1.2. Optimisation

Optimisation problems are pervasive across the financial sector, ranging from portfolio construction and risk management to liquidity allocation and operational planning. These problems often involve large numbers of variables and constraints, leading to rapidly growing computational complexity. Quantum

[5] Qubits can thus be visualized as vectors in a complex linear space, represented by two complex numbers. While a classical system occupies only one state at any given time, an n-qubit quantum system exists as a superposition of all 2^n basis states, requiring 2^n complex amplitudes to describe its full state.

[6] In particular, the famous HHL algorithm, which, under general conditions, provides exponential speedup in theory compared with classical methods

computing has been explored as a way to heuristically search for good solutions in such high-dimensional spaces.

Current research focuses on identifying problem formulations where quantum optimisation techniques can complement classical heuristics. Early experiments typically address small-scale instances and serve primarily to test algorithms and workflows rather than to demonstrate production-ready performance.

2.1.3. Quantum Machine Learning (QML)

Quantum machine learning refers to a family of approaches that seek to combine quantum computing techniques with machine learning methods. The objective is not to replace classical machine learning, but to explore whether certain sub-tasks—such as feature representation, kernel estimation or optimisation—could be enhanced using quantum resources.

2.1.4. Quantum-Inspired Methods

In parallel with developments in quantum hardware, a growing body of work has emerged around so-called quantum-inspired techniques. These methods do not actually involve proper quantum technology but draw on concepts originally developed in quantum physics, such as tensor networks, to design efficient classical algorithms for high-dimensional problems. Unlike quantum computing, quantum-inspired approaches do not require quantum hardware and can often be deployed on existing classical infrastructure.

2.2 Areas of applications

This section examines selected areas where quantum techniques, such as the above, are being investigated for their possible contribution to financial activities. The focus is not on predicting adoption or prioritising use cases, but on clarifying the nature of the problems addressed, the maturity of current approaches, and the potential system-level implications should such techniques evolve further.

2.2.1 Financial markets

Financial markets are characterised by high volumes of transactions, complex interdependencies and strong incentives for efficiency and speed. Historically, advances in computing and communication technologies have played a significant role in shaping market structures, trading strategies and regulatory frameworks. In this context, quantum technologies are being explored as a potential addition to the set of tools used in market-related activities.

Research and early experimentation have focused on several areas where quantum computing techniques may, in principle, be relevant. These include **portfolio optimisation, asset pricing and risk modelling, and the simulation of complex market dynamics**. Many of these tasks involve large combinatorial spaces or probabilistic models, which makes them computationally demanding using classical methods alone.

At present, quantum applications in financial markets remain exploratory, typically limited to small-scale or stylised instances. Classical methods continue to outperform quantum techniques in most practical settings, and any potential advantage remains highly context dependent. If, in the future,

quantum applications are widely implemented, market participants and regulators will need to consider how the adoption of the technology could potentially affect the structure of different markets, and this could have an impact on third-party and vendor dependencies.

While research suggests that quantum techniques could, over time, contribute to certain analytical or optimisation tasks, **their relevance for real-world market operations remains contingent on technological progress, governance arrangements and systemic considerations** rather than on raw computational capability alone.

2.2.2 Payment systems

Payment and settlement systems are a core component of financial stability. They are designed to operate with high levels of reliability, security and efficiency, often under strict real-time or near–real-time constraints. Even incremental improvements or disruptions in these systems can have significant implications for liquidity management, operational resilience and confidence in the financial system.

Quantum technologies are being explored in this context primarily for their potential contribution to **optimisation**, **monitoring**, and **resilience**, rather than for replacing existing payment infrastructures. Research to date has focused on whether quantum computing techniques could support specific computational tasks within payment systems that are already known to be resource-intensive when addressed with classical methods alone.

One area of interest is **liquidity optimisation** in high-value payment and settlement systems. These systems must balance the timely settlement of transactions with the efficient use of liquidity. Optimisation problems arising in this context can grow rapidly in complexity as the number of participants, transactions and constraints increases. Quantum optimisation techniques are being investigated as a possible complement to classical heuristics for exploring solution spaces more efficiently. At present, such work remains largely experimental and is typically limited to simplified or small-scale models, serving primarily to test algorithms rather than to demonstrate deployable solutions.

Another area under exploration concerns **monitoring and anomaly detection** within large-scale payment flows. Detecting unusual patterns—such as operational errors, fraud or emerging stress—requires analysing high volumes of transaction data in near real time. Quantum-assisted techniques, often combined with classical machine learning methods, have been proposed as a way to enhance pattern recognition or sampling in complex datasets. These approaches remain at an early stage, and their practical relevance depends on continued advances in both quantum hardware and hybrid algorithm design.

As in other financial domains, **potential benefits in payment systems are closely coupled with operational and integration challenges**. For the foreseeable future, quantum technologies in this area remain primarily experimental rather than transformative.

2.2.3 Central banking analysis and operations

The potential applications of quantum technologies within central banking differ in important respects from those in financial markets or commercial financial institutions. Central banks engage in a range of

analytical and operational activities that are computationally intensive, long-term in nature, and closely tied to policy formulation, system oversight and internal operations. In this context, quantum technologies are being explored primarily as **analytical and optimisation tools**, rather than as drivers of competitive advantage.

One area of interest concerns **economic and financial modelling**. Central banks rely on complex models to analyse macroeconomic and financial market dynamics, financial stability risks. These models often involve large systems of equations featuring expectations, and certain applications such as stochastic simulations and optimisation routines can be computationally demanding. Research suggests that certain quantum computing techniques could, in principle, support aspects of these tasks, such as accelerating simulations, improving sampling from complex probability distributions, or addressing specific optimisation sub-problems. At present, however, such applications remain **largely experimental**, and their relevance depends on continued progress in hardware reliability, algorithm design and hybrid classical–quantum workflows.

A related area is **risk analysis and tail-risk estimation**. Assessing rare but severe events is a persistent challenge in financial stability analysis, particularly when historical data are limited or distributions exhibit heavy tails. Quantum-assisted sampling and generative modelling techniques are being investigated as possible ways to explore complex risk landscapes more efficiently. While early research results are of academic interest, **their practical contribution to policy-relevant analysis has yet to be established**, and significant methodological and validation challenges remain.

Beyond analytical modelling, quantum technologies may also be relevant for **operational optimisation within central banks**. Examples include optimisation problems related to liquidity management, resource allocation, scheduling of critical functions, or logistical processes such as cash distribution. These problems share characteristics with those explored in other parts of the financial sector, namely high dimensionality and complex constraints. As with other domains, current work focuses on small-scale experiments and proof-of-concept studies, with **no assumption of near-term deployment**.

Quantum-assisted machine learning is another area under exploration. Central banks increasingly use machine learning techniques for tasks such as data classification, pattern recognition and text analysis, anomaly detection and forecasting. Quantum machine learning approaches seek to investigate whether quantum resources could enhance specific components of these workflows, for example through alternative data representations or optimisation steps. At present, **quantum machine learning remains at an early research stage**, and its potential benefits relative to advanced classical techniques are uncertain.

Across all these areas, **hybrid approaches combining classical and quantum computing dominate current research and experimentation**. Quantum technologies are not considered substitutes for existing analytical frameworks, but rather as possible complements that may, over time, support specific computational tasks. Integration with established systems, data governance requirements and validation standards is therefore a central consideration.

Taken together, the exploration of quantum technologies in central banking analysis and operations highlights a cautious and incremental approach. **The emphasis is on understanding potential capabilities, limitations and implications**, rather than on accelerating adoption. As with other applications discussed in this domain, the relevance of quantum technologies for central banking will

depend not only on technical progress, but also on methodological robustness, explainability and alignment with institutional mandates

2.3 System-level implications

While the potential applications of quantum technologies in finance are often examined through individual use cases, their broader implications are best understood at the level of the financial system as a whole. The effects of quantum-enabled capabilities may extend beyond isolated efficiency gains, influencing market structure, operational resilience and governance arrangements. One important consideration relates to **concentration and asymmetry effects**. If quantum technologies were to deliver meaningful advantages in specific analytical or optimisation tasks, this could reinforce existing asymmetries between institutions or contribute to concentration around a limited number of technology providers. A closely related issue concerns **shared dependencies and common points of failure**. Quantum computing resources are expected to be accessed predominantly through specialised providers, often via cloud-based platforms. Specialised providers may offer the benefits of quantum technologies to a broader range of client firms at lower costs and higher levels of quality and security than if financial firms build separate, in-house quantum capabilities. However, widespread reliance on a small number of providers, software stacks or hardware architectures, to the extent they underpin critical operations, could result in exposure to correlated risks, including technical outages, cyber incidents or supply-chain disruptions. From a system-level perspective, resilience may depend not only on the robustness of individual institutions, but also in part on the range of solution offerings within the underlying technological ecosystem.

Opacity and explainability represent another cross-cutting challenge. Some quantum techniques, particularly when combined with advanced optimisation or machine learning methods, may be difficult to interpret or validate using traditional approaches.

The **timing and distribution of impacts are also likely to remain uneven across applications and jurisdictions**, reinforcing the need to avoid assumptions of uniform or synchronised adoption. Taken together, these system-level implications suggest that the relevance of quantum technologies for the financial system cannot be assessed solely through technological performance metrics. **Issues of concentration, dependency, transparency and resilience may shape outcomes as much as computational capability itself**. Recognising these dimensions can help frame discussions on quantum technologies in a way that accounts for complexity, interdependence and uncertainty.

Synthesis

3.1 Key analytical takeaways

The analysis conducted across the two core domains of this report highlights that quantum technologies present a set of challenges and opportunities for the financial system that are defined less by immediate disruption than by potentially long uncertain time horizons and strong interdependencies.

A first key takeaway concerns the temporal nature of quantum-related risks, particularly in the area of data and communication security. The possibility that future quantum computing capabilities could compromise widely used cryptographic mechanisms represents a risk to confidentiality and integrity.

This temporal dimension, combined with the long shelf life of some types of sensitive financial data, underscores the importance of considering quantum-related risks well beyond current technological capabilities.

A second takeaway relates to the uneven maturity of quantum technologies and applications. Across both security and financial use cases, progress is highly heterogeneous. While post-quantum cryptography is advancing through standardisation and early integration efforts, other approaches, such as quantum communication techniques or quantum computing applications, remain largely experimental. In practice, most explored use cases rely on hybrid classical–quantum architectures, and their relevance depends on problem structure, system integration and operational constraints rather than on raw computational performance.

A third takeaway concerns the system-level implications associated with quantum technologies. Access to specialised computational resources and reliance on a limited number of providers may contribute to concentration effects and shared dependencies.

Finally, the analysis highlights the central role of uncertainty as a structural feature of the quantum landscape. Scientific progress, engineering feasibility and timelines for deployment remain difficult to predict, and assumptions about linear or uniform development are unlikely to hold. As a result, understanding trade-offs, limitations and alternative pathways is as important as identifying potential areas of benefit.

3.2 Skills, governance and oversight challenges

Beyond technological considerations, the exploration of quantum technologies in the financial sector raises a set of cross-cutting challenges related to skills, governance and oversight. These challenges do not constitute a separate domain of impact but rather shape how quantum-related developments are understood, assessed and managed across institutions.

Experimentation in quantum technologies currently draw on highly specialised and interdisciplinary expertise, combining elements of cryptography, cybersecurity, computer science, physics and applied mathematics. In financial contexts, this expertise must be informed by an understanding of financial infrastructures, risk management and regulatory frameworks. Differences in expertise across institutions may influence both the scope of experimentation and the ability to critically evaluate external solutions.

Governance arrangements play a similarly important role. Decisions related to quantum technologies often span multiple organisational functions, including technology, risk management, legal and policy areas. Managing these interactions requires governance structures capable of accommodating technical uncertainty while maintaining alignment with institutional mandates and risk tolerance.

From an oversight perspective, quantum-enabled techniques may accentuate existing challenges. The increasing use of complex analytical tools, particularly when combined with advanced optimisation or machine learning methods, raises questions of model transparency, validation and accountability. For supervisory authorities, assessing such tools requires not only technical understanding, but also appropriate frameworks for documentation, testing and auditability. These considerations may be further compounded when quantum-related capabilities are delivered through external providers or cross-border service arrangements.

Taken together, skills, governance and oversight challenges illustrate that the implications of quantum technologies for the financial system extend well beyond technical feasibility. They influence how risks are identified, how benefits are evaluated, and how trust and accountability are maintained as new technologies are explored.

Conclusion - Towards informed and coordinated preparedness

4.1 Reaffirming the role of informed dialogue

Quantum technologies continue to evolve in a context marked by scientific uncertainty, uneven progress and longer-term horizons. In such an environment, a shared and structured understanding of potential implications for the financial system is essential. This report has sought to contribute to that objective by considering how quantum technologies may intersect with financial infrastructures, activities and institutional frameworks.

The paper aims to clarify key issues without anticipating technological outcomes or policy decisions. A well-informed public and professional discourse can support constructive engagement, reduce the risk of misinterpretation and strengthen collective preparedness across institutions.

4.2 Looking ahead

Looking ahead, quantum technologies are likely to remain an area of sustained research and experimentation across scientific, industrial and institutional communities. Their relevance for the financial system will continue to depend on technological progress, standardisation efforts and governance practices, as well as on broader trends in digitalisation and data-intensive computing.

In this evolving landscape, preparedness is best understood as an ongoing analytical effort rather than a fixed course of action. Continued monitoring, knowledge exchange and cross-sector dialogue will remain central to informed and coordinated assessment

Appendices

2.1.5. Appendix 1 - Complementary quantum-safe approaches

In addition to post-quantum cryptography, a number of other approaches are being explored to enhance the security of data and communications in the presence of potential quantum-enabled threats. These approaches differ in their underlying principles, technical maturity and deployment models, and may complement cryptographic solutions in specific contexts rather than replace them.

One such approach is Distributed Symmetric Key Exchange (DSKE). DSKE relies on symmetric cryptographic techniques, which are generally considered less affected by quantum computing than widely used public-key schemes, combined with a network of trusted components responsible for coordinating key distribution. However, maintaining adequate security margins in a quantum context may still require adjustments such as increasing key lengths and reviewing implementations. In this model, communicating parties establish shared secret keys through pre-distributed randomness and controlled exchange mechanisms, rather than through public-key cryptography.

At the same time, DSKE introduces specific operational considerations. It typically requires reliance on trusted intermediaries or service providers to manage key provisioning, coordination and lifecycle management. This raises questions related to governance, third-party dependencies and resilience, particularly in environments where high availability and fault tolerance are critical. As a result, DSKE may be more suitable for targeted use cases involving highly sensitive data exchanges, rather than as a general-purpose replacement for existing cryptographic infrastructures.

Another approach receiving attention is Quantum Key Distribution (QKD), which uses fundamental properties of quantum mechanics to enable the establishment of cryptographic keys with strong security guarantees. In QKD systems, any attempt to intercept or measure quantum states during transmission introduces detectable disturbances, allowing communicating parties to identify potential eavesdropping. Once a shared secret key has been established through a quantum channel, classical symmetric cryptographic techniques can be used to encrypt data[7].

QKD offers a conceptually distinct security model, often described as information-theoretic security under specific assumptions. However, current implementations face practical limitations. QKD deployments typically require dedicated physical infrastructure, such as optical fibre links or satellite connections, and are often constrained by distance, cost and scalability. Integration with existing communication networks can be complex, and large-scale deployment may involve significant investment and coordination. As with other infrastructure-based solutions, considerations related to interoperability, vendor ecosystems and long-term maintenance are central to assessing feasibility.

[7] In a quantum context, maintaining adequate security margins for symmetric encryption typically involves increasing key lengths (e.g. moving from 128-bit to 256-bit keys) and reviewing related implementations. Such adjustments can entail inventorying cryptographic dependencies and updating configurations where necessary.

Both DSKE and QKD illustrate that quantum-safe security is not limited to a single technological pathway. Instead, different approaches may be combined or applied selectively, depending on the sensitivity of the data, the required level of assurance, and the operational context. In some cases, layered security architectures may be considered, where cryptographic agility, symmetric encryption and dedicated secure channels are used together to enhance overall resilience.

Beyond key exchange mechanisms, other areas of research are also relevant to quantum-safe security. These include approaches aimed at protecting data during computation, such as confidential or blind quantum computing, as well as the use of quantum-enabled sensing technologies that may affect the detection of interference or tampering in communication systems. While many of these techniques remain at an early stage, they highlight the breadth of ongoing exploration in response to quantum-related security challenges.

Taken together, these complementary approaches underscore that enhancing quantum resilience involves trade-offs rather than universal solutions. Differences in maturity, cost, scalability and governance requirements mean that the suitability of each approach must be assessed in context. Understanding these characteristics is therefore an important element of evaluating how quantum technologies may interact with the security foundations of the financial system.

2.1.6. Appendix 2 - Cross-cutting considerations

The security implications of quantum technologies for data and communications cannot be fully understood through individual technologies or use cases alone. They are shaped by a set of cross-cutting factors that influence how quantum-safe approaches are assessed, deployed and sustained across complex financial infrastructures. These factors relate in particular to interoperability, operational dependencies, governance arrangements and the availability of relevant skills.

Interoperability and transition complexity represent a central consideration. Financial systems are highly interconnected, often involving multiple institutions, infrastructures and service providers operating across jurisdictions. Cryptographic mechanisms are deeply embedded in protocols, software components and operational workflows. As quantum-safe approaches are introduced, systems relying on different cryptographic standards or security architectures may need to coexist for extended periods. Ensuring secure and reliable interaction between such systems is therefore a key challenge, particularly during transitional phases where legacy and updated components operate in parallel.

Operational dependencies and third-party risk are another important dimension. Many quantum-safe approaches, whether cryptographic or infrastructure-based, rely on external vendors for implementation, maintenance or key services. This includes software libraries, hardware components, communication infrastructure and specialised service providers. As a result, choices related to security technologies may influence dependency structures, concentration risk and resilience to disruption. Assessing these dependencies requires attention not only to technical performance, but also to governance models, contractual arrangements and the long-term sustainability of vendor ecosystems.

Cryptographic agility and governance also play a critical role. Given ongoing research in both classical and quantum cryptanalysis, no cryptographic solution can be assumed to remain secure indefinitely. The

ability to adapt security mechanisms over time, by updating algorithms, parameters or implementation, is therefore an important property of resilient systems. This agility is influenced by design choices made at the architectural level, as well as by institutional governance processes that determine how changes are assessed, tested and deployed. Clear roles, decision-making structures and coordination mechanisms can support more effective management of cryptographic evolution.

Skills and operational readiness constitute a further cross-cutting challenge. Quantum-safe security involves expertise spanning cryptography, cybersecurity, systems architecture and, increasingly, quantum technologies themselves. Such interdisciplinary skill sets remain scarce, and demand is expected to grow as quantum-related considerations become more prominent. Beyond technical expertise, organisations also require operational capacity to inventory cryptographic dependencies, monitor emerging risks and manage complex transitions. Limitations in skills and resources may therefore shape both the pace and scope of adoption.

Taken together, these cross-cutting considerations highlight that quantum-related security is not solely a technical issue. It is closely linked to organisational, operational and governance factors that influence how risks are assessed and managed across the financial system. Understanding these dimensions can help frame discussions on quantum resilience in a manner that accounts for complexity, interdependence and uncertainty, without presuming uniform solutions or trajectories.

2.1.7. Appendix 3 - Cross-cutting considerations

Appendix 3 provides a non-exhaustive and purely informational overview of selected quantum algorithms frequently referenced in the academic literature. The table does not imply practical applicability, technological readiness or near-term deployment in financial contexts. It is intended solely to support technical understanding of concepts that are commonly discussed in relation to quantum computing research.

Algorithm	Primary objective	Relevance	Maturity status
Shor's Algorithm	Efficient factorisation and discrete logarithms	Threat to RSA, ECC and related public-key systems	Theoretical; requires fault-tolerant quantum computers
Grover's Algorithm	Quadratic speed-up for unstructured search	Impacts symmetric cryptography key length considerations	Theoretical; limited by hardware scale
HHL (Harrow–Hassidim–Lloyd)	Solving linear systems of equations	Theoretical interest for financial modelling and risk analysis	Experimental; strong constraints on input/output
Quantum Amplitude Estimation (QAE)	Improved sampling and probability estimation	Monte Carlo simulations, risk estimation	Experimental; strong assumptions on data encoding and matrix properties

Quantum Approximate Optimisation Algorithm (QAOA)	Combinatorial optimisation	Portfolio optimisation, resource allocation	NISQ-era experimental research
Quantum Annealing	Heuristic optimisation	Scheduling, portfolio problems	Commercially available hardware (limited scope)
Quantum Machine Learning Algorithms (various, e.g. QSVM)	Kernel methods, feature mapping	Pattern recognition, anomaly detection	Highly experimental
Tensor Network Methods (quantum-inspired)	Efficient classical approximation of high-dimensional systems	Optimisation, ML	Classical; already deployable